Data Security: What's Old Is New Again

Data Security Takes on Greater Significance in the Age of Generative AI

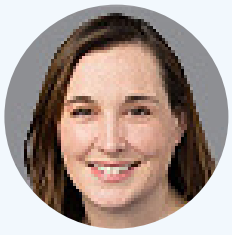
Generative AI (GenAI) has hit organizations of all sizes like a tidal wave. With rapid adoption throughout 2023, organizations saw their data security technologies in a renewed light.

Data security doesn't adhere to the same principles of other cybersecurity technologies where risky attack-like behavior and threats are "bad" and can be acted on with confidence. Data is just data. The risks to data are conditional, depending on how and where it's used, who (or what) is using it, and when. This puts an incredible onus on data security teams to create policies that control access and usage.

44.6%

According to IDC's September 2023 Future of Enterprise Spending and Resiliency Survey, 44.6% of respondents identified as a digital-native or mostly digital business. This transformation fundamentally changed the relationship enterprise organizations had with their data.

Information protection technologies have historically been implemented to control the use and spread of sensitive data beyond the organization. This provided enough visibility into data movement to offer adequate protection and compliance with industry standards. However, as digital transformation took hold, the overabundance of information became a burden. False positives increased and risks and threats were overlooked in the deluge of information.



Analyst Insight

"As enterprises outline GenAI use cases, the security and privacy of data must be a priority. Organizations should rethink and prioritize what data is most important to their business and closely control use of that information across all applications of GenAI."

Jennifer Glenn, Research Director, IDC Security and Trust

Existing Data Challenges Are Amplified

The inability to control and adequately enforce GenAI usage is becoming one of the biggest hurdles to adoption.

The business optimization/innovation versus security cycle has played out for decades. New technology comes to market, promising a better way to do business. Organizations start implementing these technologies, but security risks/problems manifest. Risks are weighed, business continues with the new technology, and security teams adjust and hope for the best. Repeat forever.

Break the Security Cycle

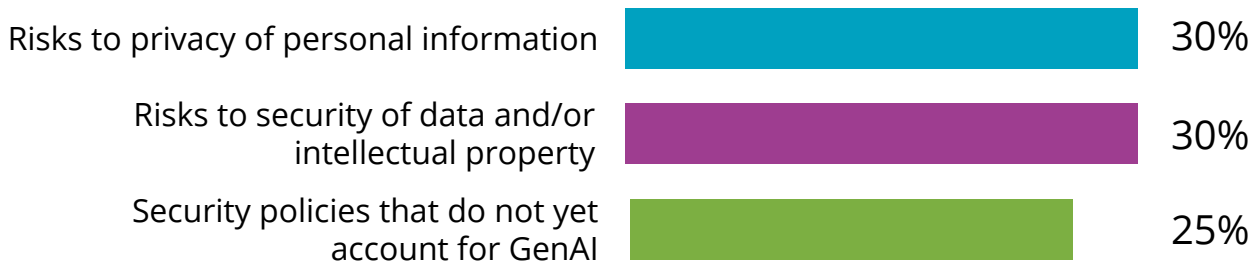
Educate
Educate users on security and privacy risks associated with sharing sensitive data to GenAI models.

Create
Create a baseline of GenAI activity to see what tools and prompts are in use.

Expand
Expand usage of existing tools to log and enforce data security policies for GenAI.

According to IDC's September 2023 Future Enterprise Resiliency and Spending Survey, 36% of worldwide respondents indicated they have put guidelines in place to allow limited use of GenAI. However, even with guidelines in place, organizations are struggling with enforcement.

Top 3 Security and Privacy Concerns With GenAI



New Data Security Challenges Are Added to the Mix

GenAI has introduced several new data security challenges including:

- **Creation of sensitive data.** Even if organizations are careful with their classification and enforcement policies, GenAI can combine public or nonvaluable data to create something sensitive or confidential.
- **Data poisoning.** If source data is not protected appropriately, it may be maliciously or even inadvertently compromised, deleted, and/or manipulated in a way that affects the output.
- **Corrupted learning.** Since most GenAI models are not trained to forget, there is a risk of poisoned, sensitive, or confidential data "living forever" in the learning output — even if the data is removed.
- **Privacy and compliance risks**. Security risks create more work for privacy and compliance professionals. With more data being generated and shared around the organization, data minimization efforts will become even more challenging.

As GenAI continues its sweep through the enterprise, data security technologies take on new focus as a means for not only protecting the 'crown jewels' but by also helping insulate the organization from new risks. Security teams want to say 'yes' to GenAI but need to prepare appropriately. Data loss technologies and data governance solutions that rely on discovery and classification to identify and categorize sensitive data are much more significant.

But, the GenAI benefits are clear: unlock the value of this far-flung data by bringing it together instantly and with minimal effort. Data can be shared in new ways across departments and business units. Customers can have more personalized engagement and experience. Repetitive tasks can be automated and/or performed faster than ever.

Source: IDC Perspective: "The Renewed Significance of Data Security for GenAI Initiatives", IDC #US51533624, January 2024

Learn more about IDC's comprehensive GenAI coverage on our AI Everywhere website. Or, connect with one of our experts and become a client.